Previous Page | Next Page

Windows 2000 Authentication

Authentication is performed by the system to be sure the user is really who they claim to be. Authentication may be done at and for a local computer or at a global level for a domain using domain controllers across the network. Windows 2000 supports the following types of authentication:

- **Kerberos V5** (RFC 1510) - An internet standard authentication protocol which is the default protocol for Windows 2000 computers within a domain. This is not used for computers in different forests.
- **Windows NT LAN Manager (NTLM)** - Used to authenticate users from Windows 95, 98, and NT systems. Windows 2000 Active Directory must be operating in mixed mode to use this authentication method.
- **Secure Sockets Layer/Transport Layer Security (SSL/TLS)** - Requires certificate servers and is used to authenticate users that are logging onto secure web sites.
- **Smart card** - Contains a chip with information about the user along with the user's private key. A personal identification number (PIN) is normally required to be authenticated using a smart card. Requires Extensible Authentication Protocol (EAP) to be enabled for the server to allow smart card authentication. Also some certificate authority must provide keys.

Authentication uses X.509 standard and kerberos.

Process of Logging On

1. CTRL+ALT+DEL is pressed, name and password entered, and local or domain logon is indicated.
2. If the logon is local, the name and password are checked against the local database. If the logon is a domain logon, the name and password are encrypted into a key, and timestamp information is encrypted. This information is sent to the Windows 2000 domain controller with an authentication request.
3. The domain controller decrypts the information and checks for a valid timestamp. If the timestamp is valid, two Kerberos tickets are made and encrypted with the password. The tickets are sent back to the client computer. The tickets are:
   - User session key - Used to log on.
   - User ticket - Used to get other Kerberos tickets for accessing other domain resources.
4. The client decrypts the tickets and uses the session key to log on.

Authentication when Accessing an Object

1. The user tries to access the network object.
2. The user ticket, user name, name of the object to access, and timestamp, are sent with a Kerberos ticket granting service request to the domain controller.

Exhibit A

3. The domain controller decrypts the information, checks the timestamp, makes an encrypted session key (with user account and group information) and returns the key to the local client.
4. The client sends a request for the resource with the session key to the the server that has the resource.
5. The receiving server decrypts the session key, and checks the information against its ACL for the object being requested.

Shares used for logon

NETLOGON/SYSVOL - The Netlogon share is used on Windows NT domain controllers to authenticate users. In Windows 2000, the SYSVOL share carries out these functions. The SYSVOL share includes group policy information which is replicated to all local domain controllers.

51. Routing
52. IPSec
53. ICS
54. Fault Tolerance
55. Backup
56. System Failure
57. Services
58. Remote Access
59. WINS
60. IIS
61. Certificate Server
62. Terminal Services
63. Web Services
64. Authentication
65. Accounts
66. Permissions
67. Groups
68. User Rights and Auditing
69. Auditing
70. User Profiles
71. Policies
72. Group Policies
73. Miscellaneous
74. Terms
75. Credits

Windows Operating Systems Home